States of Jersey

Online Safety

Policy and Procedure for

The Department of Education

Issued September 2018 *V2*

Introduction

The purpose of the online safety policy is to highlight schools, schools services and youth service safeguarding obligations, and good practice in keeping young people safe online in a technologically deterministic world.

This policy is aimed at all (School, school services and youth service Employees, including volunteers and the board of governors).

Online Risks

The internet and constantly evolving technology has changed the way that children interact with the world. While this can offer opportunities to learn and express their creativity, this technology also offers news risks such as:

- Exposure to inappropriate material (either accidentally or deliberately);
- Cyber bullying;
- Exposure to online predators;
- Sexting;
- Trolling;
- Revealing too much personal information;
- Radicalisation.

Learning to recognise warning signs will allow trusted adults to intervene where appropriate and to lessen the impact of potential negative experiences. It is vital for **ALL STAFF** to stay well informed about the issues relating to what children are experiencing using social networking, webcams, blogs, instant messaging etc.

Definitions

Throughout this policy, the word 'School' should be taken to also signify Youth Centres, Nurseries and any other educational setting.

Safeguarding

Online safety is not purely about technology. For example, if a child types a concerning word into Google, the response would be no different than if they had written it in their Mathematics book. Many of the issues arising in online safety are behavioural and will be managed in the same way as in any other area of school life. Therefore, this policy should be read in conjunction with the Child Protection Policy and other safeguarding policies. Furthermore, any escalation or response should be joined up with any other safeguarding escalation procedures.

Traditional e-Safety messages such as 'don't post personal information online' (the 'just say no' approach) are now almost meaningless as the whole point of social media for many young people is to share personal

information. Additionally, the huge range of online applications now used means that locking information down via privacy settings is almost impossible.

A more realistic and pragmatic approach is to **encourage a culture** where children and young people **feel able to share concerns with a trusted adult**, and discuss online safety issues openly. They should be encouraged to consider the scope of the potential audience to whom they are posting, the context they are posting in and to take responsibility for any potential consequences. They should understand that nothing put online can ever truly be considered 'private.'

Schools' responsibilities

Schools have a duty of care to assess and prevent possible harm to children and young people. In terms of online safety, schools have a duty to:

- **Oversee and monitor the safe use of technology when children are in their care and take action immediately if they are concerned about wellbeing;**
- **Ensure that all staff receive appropriate online safety training that is relevant and regularly updated;**
- **Ensure there are processes and mechanisms in place to support young people and staff facing online safety issues and these are publicised and transparent for young people to follow;**
- **Implement online safety policies and acceptable use policies, which are clear, understood and respected by all;**
- **Educate young people, parents and the school community to build knowledge, skills and capability in online safety;**
- **Monitor how the school is portrayed online by parents, children and staff - and demonstrate how this is monitored;**
- **Not request a website/ digital application or software to be unblocked or installed unless a risk assessment or performa has been completed;**

Schools should ensure that all children in their care are aware of their responsibilities around appropriate use of technology both inside and outside of school.

This awareness should be delivered in lessons, assemblies, events, newsletters and through the development of a culture of online safeguarding.

Schools should pro-actively engage parents and carers about online safety and related issues.

Conduct for Staff

Staff must:

- Monitor and promote positive online safety, through the use of Impero or other management software and classroom management;

- Act on and escalate all online safety issues promptly and escalate to the designated online safety individual in the school in accordance with the Child Protection and other Safeguarding policies;
- Sign a responsible use agreement and adhere to the responsibilities set out therein;
- Only use work email address to communicate with children (not personal email);
- If working remotely from home: do not divulge the password to any family members or let any member of the household use the login, laptop or device for any purpose whatsoever; use a designated room or space to work from; keep the device locked up and secure at all times;
- Use every appropriate opportunity to link online safety into the everyday curriculum;
- **Encrypt personal data** (especially if transferring information, this should be via encrypted USB or encrypting software);
- Only use websites and web based applications with students when they have been risk assessed and you have read and reviewed the terms and conditions and are satisfied that they do not pose a significant online safety or data protection risk;
- **Not** allow anyone else (whether children or other members of staff) to use their log on details or leave their computer or device unattended when logged into;
- **Not** send friend requests to (or accept friend requests from) students on social media platforms. It is acknowledged that sometimes this is complicated due to relatives etc. however caution should always be exercised in respecting professional boundaries;
- **Not** attempt to compromise or bypass online safety measures for the sake of expedience or convenience.

Designated Online Safety Individual in School

All schools must have a member of staff with designated online safety responsibilities. It is important to bear in mind that **this is primarily a safeguarding role, not an IT role**, and this member of staff should receive appropriate child protection training and be provided with sufficient time and resources to deliver their function. This **individual must also be of sufficient seniority to challenge other staff members if they are in breach of policy.** The school must update the CYPES Department of any changes to the designated Online Safety individual.

This individual will be responsible for:

- Ensuring that children are educated about online safety and related issues;
- Monitoring online activity of children;
- Escalating safeguarding concerns where appropriate if there are safeguarding concerns, within the school and to the CYPES Department and other agencies such as MASH where appropriate;
- Maintain a log of online safety incidents in the School along with any follow up;

- Be responsible for approving and risk assessing the use of any web based applications that staff wish to use;
- Reviewing school online safety and practice. It is recommended that the school uses the 360 degree safe tool **www.360safe.org.uk;**
- While this individual will be central, **all** members of staff have a responsibility to be alert to online safety risks and know how to escalate concerns appropriately. Safeguarding is everyone's responsibility;
- It is expected that students' online safety is monitored during lessons. This should most commonly be adhered to by using the Impero software system.

Internet Filtering and blocking

States Schools have their internet content filtered centrally by the CYPES Department. This will remove the majority of undesirable content but it is important to bear in mind that ***no filtering system is infallible*** and some unpleasant content will inevitably sometimes get through. This is particularly true of image searches, where some unpleasant images are tagged with innocuous words.

Therefore, you need to ensure there is sufficient supervision in place, and that your school engenders a culture where children feel they can approach a trusted member of staff if they have seen anything which worries them.

The **Impero system**, now available to all Secondary schools, **must be installed on all teacher and student computers.** It is expected that regular reports are run on the use of the system and any safeguarding, well-being or online safety issues are then discussed between the appropriate staff. An appropriate retention schedule for this information would be three months.

Staff accounts have much less filtering applied than student accounts. Again, you can apply for sites to be unblocked to staff accounts via the Helpdesk, once a performa or risk assessment has been completed.

Please note that many digital 'apps' are able to circumvent the central monitoring and filtering and vigilant monitoring of this needs to be undertaken.

Requesting a website to be blocked or unblocked or making a change request on the Helpdesk

Website unblocking. *It is the responsibility of the requesting school* to ensure that they do not make a Helpdesk request to unblock a website, until they have a) Established that it has a legitimate business or educational purpose b) Impact assessed the content of the site for suitability for the age and profile of the children who will be seeing it. This rationale and risk assessment should be documented and retained within the school and periodically reviewed. If you request for a site to be blocked, the school should continue to check periodically that the content is still inaccessible. The Digital App or Software/New Technology performa should be completed.

Change requests. If your school wants to make a request to install an application or change a configuration, or any other 'change' to the default curriculum network, you can request this via the Helpdesk. Again, schools should take responsibility for impact assessing the consequences of any such change and of any online safety or data protection implications, *before* making such an application. The 'New Technology performa' should be completed alongside the initial ticket.

Monitoring

It is the responsibility of schools to monitor young people's online behaviour in school (and to be vigilant to their online behaviour outside of school where it affects their safety or the safety of others).

Technical monitoring software provides an important opportunity to 'overhear' issues of concern, and intervene where appropriate to avoid a negative or tragic outcome.

In order to help with this, the Children, Young People, Education and Skills Department distributes daily reports to States schools about the **'suspicious search queries'** made on Google the previous day. It is important that a **designated individual in your school checks these reports daily**, and that the task is delegated in their absence. Failure to act promptly could have tragic results. Spot check searches are undertaken by the Department and if there are searches of concern the school in question will be contacted.

However, the Department will provide only basic flags about Google. For this reason, many schools also have internal monitoring systems, such as Impero, to check on all online activity. These systems are much a much more granular classroom management tool and allow you to see inside draft emails, and word documents for example. In the UK, internal school technical monitoring is a legal requirement. It is also an Ofsted recommendation that online safety is devolved to all staff and an internal monitoring tool gives you the means to do this.

Issues you should be monitoring for include (but are not limited to):

- Self-harm
- Eating disorders
- Bullying
- Pornography
- Radicalisation
- 18 rated games and films

The nature of technical monitoring software is that there will be many 'false positives' (such as 'moby dick'). *However it is very important that you do not dismiss all of the flags on this basis,* as some will be genuine.

It is for the school (and the staff who know the child) to make a judgement in context, taking into account the age, profile and background of the child, when considering how to proceed with an online concern. If there are ongoing child protection meetings then any observations of online activity should be documented and integrated into this.

Managing systems

Schools must:

- Manage and maintain different user profiles for web filtering to ensure all children are protected to an appropriate level.
- Task an individual with responsibility for managing requests to the Department's Helpdesk. This individual must be highly aware of online safety and data protection issues, so that no inappropriate requests are made.
- Monitor the selection of web based services chosen by staff, check they are risk assessed in terms of online safety and data protection - and challenge where appropriate.
- Convey clear messages to all staff and students connecting to 3G and 4G networks and unsecured domestic Wi-Fi networks, that this will bypass safeguarding filters in place when using them.
- Ensure personal information/special category information (previously referred to as sensitive data) is encrypted or password protected. This is especially important when/if information is transferred. The device information is transferred on should also be protected.
- Monitor the school's online profiles and reputation, including on unofficial sites.
- Conduct regular testing to ensure blocked content is still inaccessible.

Web histories

For children

For safeguarding reasons, it may occasionally be deemed necessary to look at the web history of a child. You can raise this request as a Helpdesk ticket - but do not name the child in the ticket- ask for a call back. The search and the reasons for the report should be documented in the child's file, and the outcome of the report integrated within any other child protection procedures.

For staff

On some occasions it will be legitimate to carry out a web history search for a member of staff. This maybe a formal request as part of a disciplinary procedure or similar. All requests should be from the Head teacher, the Police or to complete a statutory function.

Mobile devices

Mobile devices accessing the internet via the 3G or 4G networks are not subject to the same filtering and monitoring that the school systems are. This means that these devices could potentially give access to unsuitable content while on school grounds and under school supervision, not only to the owner of the device but also to their peers.

You will need to educate your learners of the potential impact to well-being of this.

If your school allows children to bring mobile devices to school you must have an in school policy in place governing their safe and responsible use. There should also be a signed agreement with students and parents as to how the device should and shouldn't be used.

Social Media

Social media is recognised as a particular risk area for children. Unlike in recent years, where young people would be on one platform, young people use a wide variety of online platforms to share personal content. This can mean that any risk and issues are more complex.

Age restrictions. Under U.S. Law a child must be minimum age 13 to use social media platform. Under the Data Protection 2018 Legislation, the Information Society has been introduced; this includes when offering an online service directly to a child, in the UK only children aged 13 or over are able provide their own consent.

Bear this in mind when asking children to use social media as part of their learning. Below are the age restrictions for the most common sites:

13: Twitter, Facebook, Instagram, Pinterest, Google+, Tumblr, Reddit, Snapchat, Secret

14: LinkedIn

16: WhatsApp

17: Vine, Tinder

18: Path

18 (but 13 with parent's consent): YouTube, Keek, Foursquare, WeChat, Kik, Flickr

All staff should ensure that their personal Social media profiles should be locked down and no publicly viewable, for example which school they work at; bearing in mind that default privacy settings change regularly and that there is really is no such thing as 'private post' on social media.

Staff should not 'friend' or accept friend requests from students on their personal social media profiles (even after they have left school, until they are 18).

If parents or members of the community post negative comments about the school or staff students in the school, DO NOT respond but instead escalate to the Headteacher who should seek advice from the Head of Governance at the Department.

Cyber-Bullying

Bullying is behaviour that is deliberate, repeated more than once and is designed to be hurtful. This type of behaviour can happen both on and offline (and often both), so it is crucial to consider all surrounding behaviour.

The impact of online bullying. While cyber-bullying can be an extension of face-to-face bullying, it differs in several significant ways: the invasion of home and personal space; the difficulty in controlling the scale and scope electronically circulated messages; the size of the audience; perceived anonymity; and even the profile of the person doing the bullying and their target is often different to 'offline' bullying.

Policies and signposts for reporting. Schools must have anti-bullying policies which articulate that participating in such activity will not be tolerated, and provide clear guidance as to who a child should contact if they feel that they or someone else is being bullied.

Support for the target. The target of cyberbullying may be in need of emotional support. Key principles here include reassuring them that they have done the right thing by telling someone; recognising that it must have been difficult for them to deal with; and reiterating that no-one has a right to do that to them. Refer to any existing pastoral support/procedures for supporting those who have been bullied in the school, and refer them to helpful information and resources.

Advice for the target. It is important to advise the person being bullied not to retaliate or return the message. Replying to messages, particularly in anger, is probably just what the bully wants, and by not replying the bully may think that the target did not receive or see the message, or that they were not bothered by it. Instead, the person should keep the evidence and take it to their parent or a member of staff Advise the pupil to think about the information they have in the public domain and where they go online. Advising the child to change their contact details, such as their Instant Messenger identity or mobile phone number, can be an effective way of stopping unwanted contact. However, it is important to be aware that some children may not want to do this, and will see this as a last resort for both practical and social reasons.

Consider bystanders. In cyber-bullying, bystanders can easily become perpetrators – by passing on or showing to others images designed to humiliate, for example, or by 'liking' or commenting on a post. They may not recognise themselves as participating in bullying, but their involvement compounds the misery for the target. It is recommended

Contain the incident. Some forms of cyberbullying involve the distribution of content or links to content, which can exacerbate, extend and prolong the bullying. It is challenging to contain this when the content may be spread across numerous sites and networks. The quickest and most effective route to getting inappropriate material taken down from the web will be to have the person who originally posted it remove it. If you know who the person responsible is, ensure that they understand why the material is hurtful and ask them to remove it. If this is unsuccessful contact the Head of Governance at the CYPES Department who will assist you in contacting the Internet Service Provider to remove the content.

Involve the wider community. Schools are advised to provide parents and carers with information about cyber-bullying policies, procedures and activities, and opportunities for becoming involved.

Self-harm

Data from the National Self-harm Registry has shown that the average person-based rate of self-harm among 10-24-year olds was 318 per 100,000. Peak rates were observed among 15-19 year old females (564 per 100,000) and 18-22 year old males (448 per 100,000). Between 2007 and 2017, rates of self-harm increased by 23%, with increases most pronounced in females and those aged 10-14 years. There were marked increases in specific methods of self-harm, including those associated with high lethality.

A Journal of Adolescence report, 2017 suggests the role of the Internet has a significant factor in young people self-harm. The report highlighted three sections contributing to an increase in self-harm. This included the use of the Internet for research into self-harming practices, exploring online imagery and exposure to such images and the distinct appeal of different social media platforms for young people engaging in self-harm.

There is also a phenomenon where some young people set up new ids online in order to send themselves bullying messages- a type of digital self-harm. This issue should be considered in conjunction with the Self Harm Policy.

If a young person is considering harming themselves, they may go online to search for methods. If your monitoring software flags up a term relating to self-harm, this must be responded to as a matter of urgency, in line with Child Protection procedures.

Radicalisation

Definition. Paragraph 7 of the Prevent Duty (UK Government advice for schools) defines extremism as: *'vocal opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs. We also include in our definition of extremism calls for the death of members of our armed forces.'*

Statutory requirements in the UK. As a result of the Counter –Terrorism and Security Act 2015, specified authorities (including schools) in the UK have a duty to have 'due regard to the need to prevent people from being drawn into terrorism.' This duty includes technical monitoring for signs of radicalisation.

Does this affect Jersey? Extremist groups aim to target young people who are perhaps lonely, disenfranchised and want to feel part of a community. This can happen to any child of any background, in any geographical location who is using the internet, and Jersey is not immune.

Sexting

Definition. Sexting is a term which describes the sharing of intimate images with others, using online technologies. Sexting is an increasing phenomenon among children, even of primary age.

The Law. Creating or sending an intimate photo of a minor (if reported as a complaint by the police) is technically a criminal offence, so incidents need very careful management.

Response. If a device is involved, secure it and switch it off. Seek advice and report to your designated safeguarding officer who should follow normal child protection procedures. Factors which would be taken into account in responding to sexting incidents include: the age of the person sending the photograph and the age of the person it was sent to; whether the individual was co-coerced into sending the image; to what extent the image has been shared online and whether the child is vulnerable and if there are existing concerns.

18 rated games and films

There is a growing phenomenon of children playing adult rated first person games such as Call of Duty or Grand Theft Auto. These games contain extreme violence, sexually explicit content, images of drug taking and

other adult themes. In addition, children have access to adults from all over the world via the headset and multi-player options, which creates an added risk.

Research shows that parents often buy these games for their children, so working in partnership with parents and carers is crucial in tackling this issue.

Online Activity Concerns

A child's behaviour online does not exist in a vacuum. It is often an extension of their situation offline. Therefore it is vital to consider online behaviour in the context of the child' situation in general and any existing concerns.

Although IT expertise is helpful in investigating or obtaining a 'red flag' about a problem, do not forget that the underlying issue is **not IT**, but safeguarding.

Therefore, you should use the same criteria as for any other Safeguarding concern.

Depending on your level of concern (and the background) it may be appropriate to make a MASH Enquiry, escalate to the CYPES Department and another agency.

There is a distinction between the kind of online activity which might result in a sanction (for example typing in swear words) and the type of activity (e.g. self-harm ideation) which calls for entirely different and considered approach and a high degree of judgement and sensitivity.

If you find illegal content

If you find illegal or potentially illegal content on the schools' network or a school owned device, you must *immediately* close down the machine, secure the room or area and seek the advice of the Headteacher immediately. The Headteacher should then contact the Head of Governance or Head of Inclusion at the CYPES Department who will provide further advice and facilitate contact with the Police.

Do not forward, copy, print or save what you have found as this could potentially be a criminal act (i.e. making indecent images) and lead to a prosecution. The police will review the material and take appropriate action.

Images of Children (photos and video)

Parental consent to publish pictures. A school must obtain parental consent to publish a picture of a child, whether on paper or online. If you fail to do this then the Department for Education could be liable for prosecution.

Consent forms. Schools should have consent forms which record parental consent to publish pictures of their child. This form should be completed at the beginning of the child's school career and can last for the duration of their time at the school. It does not have to be updated yearly however a parent has the right to change their mind and you must record that decision.

It is too vague to have a 'catch all' statement to record consent for everything though. Your consent form should be split down in sections for example:

- Use on school website/ prospectus
- Printing in the Jersey Evening Post / local media
- Social media

If there is a 'one off' reason to publish a child's picture (for example a specific event such as a royal visit) then you should seek specific consent for that event. Once the press image has been captured with consent, the media organisation is then the data controller for that image.

Other legitimate use of images in schools and guidance

Parents and carers can take pictures of their own children at their school provided it is for their own personal use and not uploaded to social networking sites.

Staff / volunteers can take pictures to support educational aims, but must follow school policies regarding the sharing, distribution and publication of those images. The images should only be recorded on school owned devices, not personal devices.

Care should be taken that students are appropriately dressed and are not participating in activities that might bring the school into disrepute.

Students must not take/use/share pictures of other students without permission.

Photographs published on the school website or elsewhere on behalf of the school will be selected carefully and appropriate consent sought.

Data Protection and social media. Care should be exercised when publishing pictures on social media. If you have gained permission from parents you are able to use a child's image in a social media post, but you need to be careful not provide more than two pieces of identifiable data, for example if the child is in school uniform and has their first name this counts as two pieces of data. You may be at risk of breaking data protection law if you post on social media and therefore care needs to be taken. It is recommended that if your school has a social media presence, you should use generic or non-identifiable group pictures.

What if there is a dispute over consent? If one parent gives consent and the other does not, you should proceed as if no consent has been given. N.B. you must have legal parental responsibility to give consent.

Web based applications. Don't forget that if you use photo or video streaming applications such as Skype, the school could effectively sharing a child's image with a third party and you should also seek consent for this.

Please refer to the Data Protection Policy for related advice on this issue.

Online safety compliance check list?

- Are you writing new and updated polices and distributing them?
- Are you involving all of your staff in online safety and training them where appropriate? DO all staff see online safety as their responsibility?
- Are you making use of filtering and monitoring software?
- Are you engaging parents, carers and the wider community?
- Are you maintaining accurate records of online safety incidents and including them on the child's file?
- Do the children in your school understand the risks around online safety and how to respond if they see anything that worries them?

Should you have any queries please contact your designated e-safety/online safety point of contact. Alternately, call the Head of Governance directly on (01534) 447864 for guidance.